Wolfgang K. Seiler
Tel. 2515

B6, B4.18

11. November 2020

7. Übungsblatt Algebra

Aufgabe 1: *(6 Punkte)*
I sei das von $f = X^2 + 2X + 2$ erzeugte Hauptideal in $R = \mathbb{Q}[X]$.

a) Zeigen Sie, daß f irreduzibel ist!

Lösung: Wenn f irreduzibel wäre, wäre es Produkt zweier Linearfaktoren aus $\mathbb{Q}[X]$, hätte also zwei rationale Nullstellen. Die Nullstellen von $f = (X+1)^2 + 1$ sind aber $-1 \pm i \notin \mathbb{Q}$. *Alternativ:* f ist 2-Eisensteinsch und damit irreduzibel.

b) Zeigen Sie, daß jede Nebenklasse $\overline{g} = g + I \in R/I$ genau ein Polynom der Form $aX + b$ mit $a, b \in \mathbb{Q}$ enthält!

Lösung: Division von g durch f führt auf einen Divisionsrest r, der entweder das Nullpolynom ist oder ein Polynom vom Grad höchstens eins. Da sich g und r durch ein Vielfaches von f unterscheiden, liegen beide in derselben Restklasse modulo $I = (f)$. Liegen zwei Polynome $aX + b$ und $cX + d$ in derselben Restklasse modulo I, ist ihre Differenz $(a-c)X + (b-d)$ durch f teilbar; da f den Grad zwei hat, ist dies nur möglich, wenn $a - c = b - d = 0$ ist und damit $aX + b = cX + d$.

c) Für die Nebenklassen $\overline{g}_1$ und $\overline{g}_2$ seien dies die Polynome $a_1X + b_1$ und $a_2X + b_2$. Finden Sie die entsprechenden Polynome für die Nebenklassen $\overline{g}_1 + \overline{g}_2$ und $\overline{g}_1 \cdot \overline{g}_2$!

Lösung: Für $\overline{g_1} + \overline{g_2} = \overline{g_1 + g_2}$ ist das natürlich $(a_1 + a_2)X + (b_1 + b_2)$. Das Produkt $\overline{g_1} \cdot \overline{g_2} = \overline{g_1 \cdot g_2}$ enthält $(a_1X + b_)(a_2X + b_2) = a_1a_2X^2 + (a_1b_2 + a_2b_1)X + b_1b_2$, aber dieses Polynom hat im Allgemeinen den Grad zwei. Division durch $X^2 + 2X + 2$ führt auf den Rest $(a_1b_2 + a_2b_1 - 2a_1a_2)X + (b_1b_2 - 2a_1a_2)$, und das ist der gesuchte Vertreter.

d) Ist R/I ein Integritätsbereich?

Lösung: Ja, denn ist das Produkt zweier Polynome aus $\mathbb{Q}[X]$ durch f teilbar, so muß wegen der Irreduzibilität von f mindestens einer der beiden Faktoren durch f teilbar sein.

Aufgabe 2: *(6 Punkte)*

a) Wie viele Elemente enthält die Gruppe $G = \big(\mathbb{Z}/16\big)^\times$?

Lösung: Eine Zahl ist genau dann teilerfremd zu $16 = 2^4$, wenn sie ungerade ist. G besteht daher aus den acht Elementen $1, 3, 5, 7, 9, 11, 13$ und 15.

b) Bestimmen Sie die Ordnungen aller Elemente von G !

Lösung: Die Eins ist das einzige Element der Ordnung eins, und $15 = -1$ hat die Ordnung zwei. Alle Ordnungen sind Teiler von 16, also Zweierpotenzen. 3^2 und $13^2 = (-3)^2$ sind neun und $9^2 = 1$, also haben 9 und $-9 = 7$ die Ordnung zwei, während 3 und 13 die Ordnung vier haben. $5^2 = 11^2 = 9$, also haben auch 5 und 11 die Ordnung vier. Damit sind alle Ordnungen bestimmt.

c) Finden Sie Elemente $a, b \in G$ derart, daß die Abbildung

$$\varphi\colon \begin{cases} \mathbb{Z}/4 \oplus \mathbb{Z}/2 \to (\mathbb{Z}/16)^\times \\ \qquad (n, m) \mapsto a^n \cdot b^m \end{cases}$$

ein Gruppenisomorphismus ist!

Lösung: Dazu muß a die Ordnung vier haben und b die Ordnung zwei. Nach *b)* ist drei ein Element der Ordnung vier und sieben eines der Ordnung zwei. Wir können es daher versuchen mit der Abbildung $(n, m) \mapsto 3^n \cdot 7^m$. φ ist ein Homomorphismus, denn

$$\begin{aligned} \varphi\big((n, m) + (n', m')\big) &= \varphi\big((n + n', m + m')\big) = 3^{n+n'} \cdot 7^{m+m'} = (3^n \cdot 7^m)(3^{n'} \cdot 7^{m'}) \\ &= \varphi\big((n, m)\big) \cdot \varphi\big((n', m')\big) . \end{aligned}$$

Ist $\varphi\big((n, m)\big) = 1$, so ist $3^n \cdot 7^m \equiv 1 \bmod 16$. Da die Sieben Ordnung zwei hat, ist sie ihr eigenes Inverses in $(\mathbb{Z}/16)^\times$, also ist $3^n \equiv 7^m \bmod 16$. Die möglichen Potenzen von drei sind 3, 9, 11 und 1; die von sieben sind 7 und 1. Ist also $3^n \equiv 7^m \bmod 16$, muß beides modulo 16 gleich eins sein, d.h. $(n, m) = (0, 0)$. Somit ist die Abbildung injektiv. Als Selbstabbildung einer endlichen Menge ist sie dann auch surjektiv, also ein Isomorphismus.
(Alternativ kann man natürlich auch durch Einsetzen aller möglicher Paare (n, m) die Surjektivität nachweisen und daraus auf die Injektivität schließen.)

d) Folgern Sie, daß $a^4 \equiv 1 \bmod 16$ für jede ungerade ganze Zahl a!

Lösung: In $\mathbb{Z}/4 \oplus \mathbb{Z}/2$ ist die Ordnung eines jeden Elements ein Teiler von vier, also auch in $(\mathbb{Z}/16)^\times$. Daher gilt für jedes Element $x \in (\mathbb{Z}/16)^\times$, daß $x^4 = 1$ ist, d.h. für jede zu 16 teilerfremde Zahl a ist $a^4 \equiv 1 \bmod 16$. (Die zu 16 teilerfremden Zahlen sind natürlich einfach die ungeraden.)

e) Gilt auch, daß $a^5 \equiv a \bmod 16$ für *alle* $a \in \mathbb{Z}$?

Lösung: *Nein;* für jede gerade Zahl ist $a^5 \equiv 0 \bmod 16$, so daß alle nicht durch 16 teilbaren geraden Zahlen Gegenbeispiele sind.

Aufgabe 3: *(4 Punkte)*

a) G und H seien zwei Gruppen mit Neutralelementen e_G und e_H. Zeigen Sie, daß die Teilmengen $N_1 = G \times \{e_H\}$ und $N_2 = \{e_G\} \times H$ Normalteiler von $G \oplus H$ sind und daß es zu jedem Element $x \in G \oplus H$ eindeutig bestimmte Elemente $n_1 \in N_1$ und $n_2 \in N_2$ gibt mit $x = n_1 n_2 = n_2 n_1$!

Lösung: $G \oplus H = G \times H = \big\{(a, b) \bigm| a \in G, b \in H\big\}$, $N_1 = \big\{(x, e_H) \bigm| x \in G\big\}$ und $N_2 = \big\{(e_G, y) \bigm| x \in G, y \in H\big\}$. Für (a, b) in $G \oplus H$ und $(x, e_H) \in N_1$ ist

$$(a, b)^{-1}(x, e_H)(a, b) = (a^{-1}, b^{-1})(x, e_H)(a, b) = (a^{-1}xa, b^{-1}e_H b) = (a^{-1}xa, e_H) \in N_1 ,$$

da $a^{-1}xa$ natürlich in G liegt. Genauso ist für $(e_G, y) \in N_2$

$$(a, b)^{-1}(e_G, y)(a, b) = (a^{-1}, b^{-1})(e_G)(a, b) = (a^{-1}e_G a, b^{-1}yb) = (e_G, b^{-1}yb) \in N_2 .$$

Damit sind N_1 und N_2 Normalteiler.
Für ein beliebiges Element $(a, b) \in G \times H$ ist

$$(a, e_H)(e_G, b) = (e_G, b)(a, e_H) = (a, b) ,$$

und das sind offensichtlich die einzigen Elemente von N_1 und N_2 für die das gilt.

b) Eine Gruppe G habe zwei Normalteiler N_1, N_2 mit der Eigenschaft, daß $N_1 \cap N_2$ eine einelementige Menge ist und es zu jedem $x \in G$ eindeutig bestimmte Elemente $n_1 \in N_1$ und $n_2 \in N_2$ gibt mit $x = n_1 n_2 = n_2 n_1$. Zeigen Sie, daß $G \cong N_1 \oplus N_2$ ist!

Lösung: Wir überlegen uns zunächst, daß für zwei Elemente $m_1 \in N_1$ und $m_2 \in N_2$ stets $m_1 m_2 = m_2 m_1$ sein muß: Zu $m_1 m_2 \in G$ gibt es nach Voraussetzung eindeutig bestimmte Elemente $n_1 \in N_1$ und $n_2 \in N_2$ derart, daß $m_1 m_2 = n_1 n_2 = n_2 n_1$ ist. Damit ist $n_1^{-1} m_1 = n_2 m_2^{-1}$. Die linke Seite liegt in N_1, die rechte in N_2; da $N_1 \cap N_2$ nur ein Element enthält, das natürlich das Neutralelement von G sein muß, folgt $n_1 = m_1$ und $n_2 = m_2$. Wegen $n_1 n_2 = n_2 n_1$ ist daher auch $m_1 m_2 = m_2 m_1$.
Betrachten wir nun die Abbildung

$$\varphi \colon \begin{cases} G \to N_1 \oplus N_2 \\ x \mapsto (n_1, n_2) \end{cases},$$

die jedem Element $x \in G$ das eindeutig bestimmte Paar $(n_1, n_2) \in N_1 \oplus N_2$ zuordnet, für das $x = n_1 n_2 = n_2 n_1$ ist. Sie ist ein Homomorphismus, denn ist $x = n_1 n_2$ und $y = m_1 m_2$, so ist $xy = n_1 n_2 m_1 m_2 = (n_1 m_1)(n_2 m_2)$, da n_2 und m_1, wie wir gerade gesehen haben, als Elemente von N_2 *bzw.* N_1 miteinander kommutieren. Somit ist

$$\varphi(xy) = (n_1 n_2, m_1 m_2) = \varphi(x)\varphi(y).$$

Ein Element $(n_1, n_2) \in N_1 \oplus N_2$ hat $x = n_1 n_2$ als Urbild, so daß φ surjektiv ist. Die Abbildung ist auch injektiv, denn ist $\varphi(x) = (e, e)$, so ist $x = ee = e$. Somit ist φ ein Isomorphismus.

Aufgabe 4: *(4 Punkte)*

a) Wie viele Elemente hat die Gruppe $G = (\mathbb{Z}/105)^\times$?

Lösung: 105 ist durch drei teilbar (Quersumme sechs) und durch fünf, also ist $105 = 3 \cdot 5 \cdot 7$ die Primzerlegung. Die Elementanzahl von $(\mathbb{Z}/105)^\times$ ist daher

$$\varphi(105) = \varphi(3) \cdot \varphi(5) \cdot \varphi(7) = 2 \cdot 4 \cdot 6 = 48.$$

b) Zeigen Sie, daß $(\mathbb{Z}/105)^\times \cong \mathbb{Z}/2 \oplus \mathbb{Z}/4 \oplus \mathbb{Z}/6$ ist!

Lösung: Nach dem chinesischen Restesatz ist $(\mathbb{Z}/105)^\times \cong (\mathbb{Z}/3)^\times \oplus (\mathbb{Z}/5)^\times \oplus (\mathbb{Z}/7)^\times$. Da für eine Primzahl p die Gruppe $(\mathbb{Z}/p)^\times$ als multiplikative Gruppe eines endlichen Körpers zyklisch ist und $p-1$ Elemente hat, ist sie isomorph zu $\mathbb{Z}/(p-1)$, d.h. $G \cong \mathbb{Z}/2 \oplus \mathbb{Z}/4 \oplus \mathbb{Z}/6$.

c) Ist $(\mathbb{Z}/105)^\times$ zyklisch?

Lösung: $(\mathbb{Z}/105)^\times$ hat 48 Elemente. Die Ordnung eines jeden Elements von $\mathbb{Z}/n$ ist ein Teiler von n; die Ordnung eines Elements von $\mathbb{Z}/2 \oplus \mathbb{Z}/4 \oplus \mathbb{Z}/6$ muß also das kgV zwölf von $2, 4$ und 6 teilen. Die Gruppe kann daher kein Element der Ordnung 48 enthalten und ist nicht zyklisch.